

## Claims

1. A method of securely implementing a public-key cryptography algorithm, the public key being composed  
 5 of an integer  $n$  that is a product of two large prime numbers  $p$  and  $q$ , and of a public exponent  $e$ , said method consisting in determining a set  $E$  comprising a predetermined number of prime numbers  $e_i$  that can correspond to the value of the public exponent  $e$ , said  
 10 method being characterized in that it comprises the following steps consisting in:

a) computing a value  $\Phi = \prod_{e_i \in E} e_i$

such that  $\Phi/e_i$  is less than  $\Phi(n)$  for any  $e_i$   
 15 belonging to  $E$ , where  $\Phi$  is the Euler totient function;

b) applying the value  $\Phi$  to a predetermined computation;

c) for each  $e_i$ , testing whether the result of said predetermined computation is equal to a value  $\Phi/e_i$ :

20 - if so, then attributing the value  $e_i$  to  $e$ , and storing  $e$  with a view to it being used in computations of said cryptography algorithm;

- otherwise, observing that the computations of the cryptography algorithm using the value  $e$  cannot be  
 25 performed.

2. A method according to claim 1, characterized in that the cryptography algorithm is based on an RSA-type algorithm in standard mode.

3. A method according to claim 2, characterized in that the predetermined computation of step b) consists in computing a value C:

5         $C = \Phi \cdot d \text{ modulo } \Phi(n)$ , where d is the corresponding private key of the RSA algorithm such that  $e \cdot d = 1 \text{ modulo } \Phi(n)$  and  $\Phi$  is the Euler totient function.

10       4. A method according to claim 2, characterized in that the predetermined computation of step b) consists in computing a value C:

$C = \Phi \cdot d \text{ modulo } \Phi(n)$ , where d is the corresponding private key of the RSA algorithm such that  $e \cdot d = 1 \text{ modulo } \Phi(n)$ , with  $\Phi$  being the Carmichael function.

15

5. A method according to claim 1, characterized in that the cryptography algorithm is based on an RSA-type algorithm in CRT mode.

20       6. A method according to claim 5, characterized in that the predetermined computation of step b) consists in computing a value C:

25        $C = \Phi \cdot d_p \text{ modulo } (p-1)$ , where  $d_p$  is the corresponding private key of the RSA algorithm such that  $e \cdot d_p = 1 \text{ modulo } (p-1)$ .

7. A method according to claim 5, characterized in that the predetermined computation of step b) consists in computing a value C:

$C = \Phi.d_q \text{ modulo } (q-1)$ , where  $d_q$  is the corresponding private key of the RSA algorithm such that  $e.d_q = 1 \text{ modulo } (q-1)$ .

5           8. A method according to claim 5, characterized in that the predetermined computation of step b) consists in computing two values  $C_1$  and  $C_2$  such that:

$C_1 = \Phi.d_p \text{ modulo } (p-1)$ , where  $d_p$  is the corresponding private key of the RSA algorithm such  
10 that  $e.d_p = 1 \text{ modulo } (p-1)$ ;

$C_2 = \Phi.d_q \text{ modulo } (q-1)$ , where  $d_q$  is the corresponding private key of the RSA algorithm such that  $e.d_q = 1 \text{ modulo } (q-1)$ ;

and in that the test step c) consists, for each  
15  $e_i$ , in testing whether  $C_1$  and/or  $C_2$  is equal to the value  $\Phi/e_i$ :

- if so, then attributing the value  $e_i$  to  $e$  and storing  $e$  with a view to it being used in computations of said cryptography algorithm;

20           - otherwise, observing that the computations of said cryptography algorithm using the value  $e$  cannot be performed.

9. A method according to claim 3 or claim 4 and  
25 in which a value  $e_i$  has been attributed to  $e$ , said method being characterized in that the computations using the value  $e$  consist in:

choosing a random integer  $r$ ;

computing a value  $d^*$  such that  $d^* = d + r \cdot (e \cdot d - 1)$ ;  
and

implementing a private operation of the algorithm  
in which a value  $x$  is obtained from a value  $y$  by  
5 applying the relationship  $x = y^{d^*}$  modulo  $n$ .

10. A method according to any one of claims 2 to  
4, and in which a value  $e_i$  has been attributed to  $e$ ,  
said method being characterized in that it consists,  
10 after a private operation of the algorithm, in  
obtaining a value  $x$  from a value  $y$ , and in that the  
computations using the value  $e$  consist in checking  
whether  $x^e = y$  modulo  $n$ .

15 11. A method according to any one of claims 5 to  
8, and in which a value  $e_i$  has been attributed to  $e$ ,  
characterized in that it consists, after a private  
operation of the algorithm, in obtaining a value  $x$  from  
a value  $y$ , and in that the computations using the value  
20  $e$  consist in checking firstly whether  $x^e = y$  modulo  $p$   
and secondly whether  $x^e = y$  modulo  $q$ .

12. A method according to any preceding claim,  
characterized in that the set  $E$  comprises at least the  
25 following  $e_i$  values: 3, 17,  $2^{16} + 1$ .

13. An electronic component characterized in that  
it comprises means for implementing the method  
according to any preceding claim.

14. A smart card including an electronic component according to claim 13.

15. A method of securely implementing a public-key cryptography algorithm, the public key being composed of an integer  $n$  that is a product of two large prime numbers  $p$  and  $q$ , and of a public exponent  $e$ , said method consisting in determining a set  $E$  comprising a predetermined number of prime numbers  $e_i$  that can correspond to the value of the public exponent  $e$ , said method being characterized in that it comprises the following steps consisting in:

a) choosing a value  $e_i$  from the values of the set  $E$ ;

b) if  $\Phi(p) = \Phi(q)$ , testing whether the chosen  $e_i$  value satisfies the relationship:

$$(1 - e_i \cdot d) \text{ modulo } n < e_i \cdot 2^{(\Phi(n)/2) + 1}$$

or said relationship as simplified:

$$(-e_i \cdot d) \text{ modulo } n < e_i \cdot 2^{(\Phi(n)/2) + 1}$$

where  $\Phi(p)$ ,  $\Phi(q)$ , and  $\Phi(n)$  are the functions giving the numbers of bits respectively encoding the number  $p$ , the number  $q$ , and the number  $n$ ;

otherwise, when  $p$  and  $q$  are unbalanced, testing whether the chosen  $e_i$  value satisfies the following relationship:

$$(1 - e_i \cdot d) \text{ modulo } n < e_i \cdot 2^{g+1}$$

or said relationship as simplified:

$$(-e_i \cdot d) \text{ modulo } n < e_i \cdot 2^{g+1}$$

with  $g = \max(\Phi(p), \Phi(q))$ , if  $\Phi(p)$  and  $\Phi(q)$  are known, or, otherwise, with  $g = \Phi(n)/2 + t$ , where  $t$  designates the imbalance factor or a limit on that factor;

5        c) if the test relationship applied in the preceding step is satisfied and so  $e = e_i$ , storing  $e$  with a view to using it in computations of said cryptography algorithm;

10        - otherwise, reiterating the preceding steps while choosing another value for  $e_i$  from the set  $E$  until an  $e_i$  value can be attributed to  $e$  and, if no  $e_i$  value can be attributed to  $e$ , then observing that the computations of said cryptography algorithm using the value of  $e$  cannot be performed.

15

16. A method according to claim 15, characterized in that, for all values of  $i$ ,  $e_i \leq 2^{16} + 1$ , and in that the step b) is replaced by another test step consisting in:

20        b) if  $\Phi(p) = \Phi(q)$ , testing whether the chosen  $e_i$  value satisfies the relationship:

$$(1 - e_i \cdot d) \bmod n < e_i \cdot 2^{(\Phi(n)/2) + 17}$$

or said relationship as simplified:

$$(-e_i \cdot d) \bmod n < e_i \cdot 2^{(\Phi(n)/2) + 17}$$

25        where  $\Phi(p)$ ,  $\Phi(q)$ , and  $\Phi(n)$  are the functions giving the numbers of bits respectively encoding the number  $p$ , the number  $q$ , and the number  $n$ ;

otherwise, when  $p$  and  $q$  are unbalanced, testing whether the chosen  $e_i$  value satisfies the following relationship:

$$(1-e_i.d) \text{ modulo } n < e_i.2^{g+17}$$

or said relationship as simplified:

$$(-e_i.d) \text{ modulo } n < e_i.2^{g+17}$$

5 with  $g=\max(\Phi(p),\Phi(q))$ , if  $\Phi(p)$  and  $\Phi(q)$  are known, or, otherwise, with  $g=\Phi(n)/2+t$ , where  $t$  designates the imbalance factor or a limit on that factor.

10 17. A method according to claim 15, characterized in that step b) is replaced with another test step consisting in:

testing whether the chosen  $e_i$  value satisfies the relationship whereby:

15 the first most significant bits of  $(1-e_i.d)$  modulo  $n$  are zero;

or said relationship as simplified whereby:

the first most significant bits of  $(-e_i.d)$  modulo  $n$  are zero.

20 18. A method according to claim 17, characterized in that the test is performed on the first 128 most significant bits.

25 19. A method according to any one of claims 15 to 18, characterized in that the cryptography algorithm is based on an RSA-type algorithm in standard mode.

20. A method according to any one of claims 15 to 19, and in which an  $e_i$  value has been attributed to  $e$ ,

said method being characterized in that the computations using the value  $e$  consist in:

- choosing a random integer  $r$ ;
- computing a value  $d^*$  such that  $d^* = d + r \cdot (e \cdot d - 1)$ ;

implementing a private operation of the algorithm in which a value  $x$  is obtained from a value  $y$  by applying the relationship  $x = y^{d^*}$  modulo  $n$ .

21. A method according to any one of claims 15 to 19 and in which an  $e_i$  value has been attributed to  $e$ , said method being characterized in that it consists, after a private operation of the algorithm, in obtaining a value  $x$  from a value  $y$  and in that the computations using the value  $e$  consist in checking whether  $x_e = y$  modulo  $n$ .

22. A method according to any one of claims 15 to 21, characterized in that the set  $E$  comprises at least the following  $e_i$  values: 3, 17,  $2^{16}+1$ .

23. A method according to claim 22, characterized in that the preferred choice of the values  $e_i$  from the values of the set  $E$  is made in the following order:  $2^{16}+1$ , 3, 17.

24. An electronic component characterized in that it comprises means for implementing the method according to any one of claims 15 to 23.



25. A smart card including an electronic component according to claim 24.